Tlf: 39 15 52 00
koebenhavn@bdo.dk
www.bdo.dk

BDO Statsautoriseret revisionsaktieselskab
Havneholmen 29
DK-1561 København V
CVR-nr. 20 22 26 70

9K TECHNOLOGIES APS

ISAE 3000-ERKLÆRING PR. 18. JANUAR 2015
OM BESKRIVELSEN AF SYSTEMER OG
DE TILHØRENDE KONTROLLER OG DERES UDFORMNING
TIL SIKRING AF OVERHOLDELSE AF LOV OM
BEHANDLING AF PERSONOPLYSNINGER

INDHOLDSFORTEGNELSE

Side

1. UAFHÆNGIG REVISORS ERKLÆRING MED SIKKERHED OM BESKRIVELSEN AF 9K TECHNOLOGIES APS' SYSTEMER OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING TIL SIKRING AF OVERHOLDELSE AF LOV OM BEHANDLING AF PERSONOPLYSNINGER

Til: Ledelsen i 9k Technologies ApS
9k Technologies ApS' kunder

Omfang
Vi har fået som opgave at afgive erklæring om 9k Technologies ApS' (serviceleverandøren) beskrivelse på side 5 af systemer og de pr. 18. januar 2015 tilhørende kontroller og deres udformning til sikring af overholdelse af lov om behandling af personoplysninger (beskrivelsen), og om serviceleverandøren i forhold til de anvendte systemer overholder lov om behandling af personoplysninger.

Serviceleverandørens ansvar
På side 4 i nærværende rapport har serviceleverandøren afgivet et udsagn om egnetheden af den samlede præsentation af beskrivelsen samt hensigtsmæssigheden af de udformede kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandøren er ansvarlig for udarbejdelsen af beskrivelsen og udsagnet, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter. Serviceleverandøren er desuden ansvarlig for at definere kontrolmål samt udforme og implementere tekniske og organisatoriske foranstaltninger (kontroller) mod, at de i systemerne registrerede personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, eller at disse personoplysninger kommer til uvedkommendes kendskabs, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om serviceleverandørens beskrivelse samt om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse, og om serviceleverandøren i forhold til de anvendte systemer overholder lov om behandling af personoplysninger.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Revisionen er tilrettelagt og udført med henblik på at opnå høj grad af sikkerhed for vores konklusion og er baseret på lov om behandling af personoplysninger, jf. lov nr. 479 af 31. maj 2000 med senere ændringer, og de i medfør af lovens udstedte bekendtgørelser, herunder bekendtgørelse nr. 528 af 15. juni 2000 med senere ændringer (sikkerhedsbekendtgørelsen).

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sine systemer samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen og hensigtsmæssigheden af anførte kontrolmål.

Vores arbejde har omfattet forespørgsler, observationer og inspektioner samt stikprøvevis efterprøvelse af den information, vi har modtaget. Det er vores opfattelse, at det udførte arbejde giver et tilstrækkeligt og egnet grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør
Serviceleverandørens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og omfatter derfor ikke nødvendigvis alle de aspekter ved systemerne, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen af personoplysninger.

Konklusion
Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i serviceleverandørens udsagn på side 4. Det er vores opfattelse:

a. at beskrivelsen af systemer og de tilhørende kontroller til sikring af overholdelse af lov om behandling af personoplysninger, således som de var udformet og implementeret pr. 18. januar 2015, i alle væsentlige henseender er retvisende,

b. at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 18. januar 2015, og

c. at serviceleverandøren i forhold til de anvendte systemer overholder lov om behandling af personoplysninger, herunder sikkerhedsbekendtgørelsen.

Beskrivelse af test af kontroller
De specifikke kontroller, der er blevet testet, og resultater af disse test fremgår på side 7-14.

Tiltænkte brugere og formål
Denne erklæring er udelukkende tiltænkt serviceleverandørens kunder, når de som dataansvarlige i henhold til lov om behandling af personoplysninger vurderer de tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med de anvendte systemer. Erklæringen må ikke anvendes til andre formål.

København, den 10. februar 2015

Per Sloth
Partner, it-revisionschef
Registreret revisor

2. UDSAGN FRA 9K TECHNOLOGIES APS

Medfølgende beskrivelse er udarbejdet til brug for de kunder, der har anvendt 9k Technologies ApS' systemer, bestående af *Borgerregnskab* og *Min Arbejdsdag*, således at disse opnår en forståelse af de til systemerne hørende kontroller og deres udformning til sikring af overholdelse af lov om behandling af personoplysninger.

9k Technologies ApS bekræfter, at:

a. Den medfølgende beskrivelse på side 5 giver et retvisende billede af systemerne *Borgerregnskab* og *Min Arbejdsdag* og de tilhørende kontroller og deres udformning pr. 18. januar 2015. Kriterierne for dette udsagn var, at den medfølgende beskrivelse:

   - Redegør for, hvordan systemerne og kontrollerne var udformet og implementeret, herunder relevante kontrolmål og kontrolaktiviteter udformet til at nå disse mål.

   - Redegør for kontroller, som vi med henvisning til systemernes udformning har været forudsat implementeret hos kunderne, for at sikre opfyldelse af lov om behandling af personoplysninger

   - Redegør for andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante

   - Ikke udelader eller forvansker information, der er relevant for omfanget af de beskrevne systemer, under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og derfor ikke kan omfatte ethvert aspekt ved systemerne, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

b. De kontroller, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 18. januar 2015.

c. De kontroller, der er anført i medfølgende beskrivelse, var tilstrækkelige til at sikre, at reglerne i lov om behandling af personoplysninger og kravene i sikkerhedsbekendtgørelsen er overholdt pr. 18. januar 2015.

Aalborg, den 9. februar 2015

9k Technologies ApS

Jonas Bruun Nielsen
Administrerende direktør

3. BESKRIVELSE AF 9K TECHNOLOGIES APS' SYSTEMER OG DE TILHØRENDE KONTROLLER TIL SIKRING AF OVERHOLDELSE AF LOV OM BEHANDLING AF PERSONOPLYSNINGER

Systemer

9k Technologies ApS' systemer består af to værktøjer: *Borgerregnskab*, som er en nemmere og tidsbesparende løsning til håndtering af beboerøkonomi, og *Min Arbejdsdag*, der er et arbejdsmiljøværktøj med fokus på at nedbringe sygefravær og øge arbejdsglæden på arbejdspladsen.

9k Technoliges ApS udvikler, vedligeholder og driver værktøjerne, der baseres på samme webapplikation og database. Opbevaring af data sker på samme platform. 9k Technologies gør brug af en serviceunderleverandør til serverdrift med henblik på at øge stabilitet og sikkerhed for fysisk adgang til data.

Det er af væsentlig betydning for 9k Technologies ApS' ledelse, at der gennem et fokus på høj it-sikkerhed sikres, at lov om behandling af personoplysninger efterleves. De trufne foranstaltninger og indførte kontroller bliver løbende vedligeholdt, og det vurderes med jævne mellemrum, om der er behov for at justere foranstaltninger og kontroller.

Identifikation af risici og implementering af kontroller

9k Technologies ApS' ledelse har analyseret de systemmæssige risici. På baggrund af risikoanalysen har ledelsen formuleret relevante kontrolmål og implementeret de nødvendige kontrolaktiviteter, således at det sikres, at systemerne overholder lov om behandling af personoplysninger og den i medfør heraf udstedte sikkerhedsbekendtgørelse.

Kontrolmål og kontrolaktiviteter er opdelt i følgende hovedområder:

- Generelle sikkerhedsbestemmelser
- Autorisation og adgangskontrol
- Ind- og uddatamateriale som indeholder personoplysninger
- Eksterne kommunikationsforbindelser
- Logning

For en nærmere beskrivelse af de definerede kontrolmål og de udformede kontrolaktiviteter, for at nå disse kontrolmål, henvises der til punkt 4.1 - 4.5, der en integreret del af nærværende beskrivelse.

Komplementerende kontroller hos kunderne

Kontroller hos 9k Technologies ApS er udformet på en sådan måde, at disse skal suppleres med kundens egne kontroller, for at sikre opfyldelse af lov om behandling af personoplysninger.

Med henvisning til sikkerhedsbekendtgørelsen skal kunden således som minimum selv indføre følgende procedurer, instrukser og kontroller i tilknytning til anvendelsen af værktøjerne:

1. Generel instruks til alle medarbejderne om behandling og destruktion af ind- og uddatamateriale samt anvendelse af værktøjerne.

2. Procedure for administration af brugere i værktøjerne, herunder oprettelse, ændring og sletning af brugere, samt tildeling af brugerrettigheder i overensstemmelse med de roller, som er oprettet i værktøjerne.

3. Kontrol af tildelte brugerrettigheder, der skal udføres mindst en gang hvert halve år.

4. Instruks for udskiftning af adgangskendeord (password) på oprettede brugere.

4. KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

I nærværende beskrivelse er følgende informationer beskrevet af 9k Technologies ApS:

- Relevante kontrolmål, udvalgt af 9k Technologies ApS.
- Indførte kontrolaktiviteter, udvalgt af 9k Technologies, og udformet til at nå kontrolmålene.

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger med henblik på at opnå høj grad af sikkerhed for vores konklusion.

Vores test af kontrollernes design og implementering har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af 9k Technologies ApS. Vores test har omfattet de handlinger, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået pr. 18. januar 2015.

I nærværende beskrivelse er følgende informationer således beskrevet af BDO:

- En beskrivelse af de udførte test med henblik på at konkludere, hvorvidt 9k Technologies ApS' anførte kontroller var hensigtsmæssigt udformet til at nå de anførte kontrolmål.
- Resultatet af vores test af hensigtsmæssighed og udformning af kontroller.

De udførte test af kontrollernes design og implementering er beskrevet nedenfor:

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale hos 9k Technologies ApS er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

For de ydelser, som Wannafind.dk A/S leverer inden for drift af systemerne, har vi fra uafhængig revisor modtaget en erklæring om generelle it-kontroller relateret til drifts- og hostingsydelser. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i 9k Technologies ApS' beskrivelse af systemer og tilhørende kontroller til sikring af overholdelse af lov om behandling af personoplysninger. Vi har således alene vurderet erklæringen og testet de kontroller hos 9k Technologies ApS, der overvåger funktionaliteten af serviceunderleverandørens kontroller (partielmetoden).

4.1 Generelle sikkerhedsbestemmelser

Kontrolmål

- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*
- *At beskytte mod tab af data.*
- *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*
- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.*
- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.1.1 Databehandlingsaftaler • Der indgås skriftlige databehandlingsaftaler mellem 9k Technologies ApS og kunderne. • Der foretages halvårlig kontrol af de indgåede databehandlingsaftaler for at sikre, at nyoprettede kunder har udfyldt en sådan aftale. Kontrollen godkendes af direktionen.	Vi har foretaget interview af passende personale. Vi har observeret, at serviceleverandøren har indført en procedure til sikring af, at der indgås skriftlige databehandlingsaftaler, og vi har foretaget inspektion af udvalgte databehandlingsaftaler. Vi har observeret, at direktionen har udført kontrollen som beskrevet i proceduren.	Ingen afvigelser konstateret.
4.1.2 Risikovurdering • Udviklingsteamet foretager årligt en vurdering af sikkerhedsmæssige risici og planlægger eventuelle muligheder for forbedring. Direktionen kontrollerer, at denne vurdering finder sted.	Vi har foretaget interview af passende personale. Vi har inspiceret den årlige vurdering af sikkerhedsmæssige risici, herunder serviceleverandørens vurdering af tekniske sårbarhed, eksponeringen og de iværksatte foranstaltninger. Vi har observeret, at direktionen har udført sin kontrol som beskrevet i proceduren.	Ingen afvigelser konstateret.
4.1.3 Sikkerhedspolitikkontrakt • Det kontrolleres årligt og godkendes af direktionen, at alle nye medarbejdere, der er en del af udviklingsteamet, har underskrevet 9k Technologies ApS' sikkerhedspolitikkontrakt.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren og de for medarbejderne oprettede sikkerhedspolitikkontrakter. Vi har observeret, at direktionen har udført sin kontrol som beskrevet i proceduren.	Ingen afvigelser konstateret.

4.1 Generelle sikkerhedsbestemmelser

Kontrolmål

- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*
- *At beskytte mod tab af data.*
- *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*
- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.*
- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.1.4 Serviceunderleverandør - ISAE 3402-erklæring • Direktionen kontrollerer, at den anvendte serviceleverandør årligt fremlægger en opdateret ISAE 3402-erklæring, som gennemlæses og kontrolleres med henblik på at konstatere, om serviceleverandøren stadig lever op til 9k Technologies ApS' krav til håndtering af produktionsserveren.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren og den indgående hostingaftale for drift af produktionsserveren. Vi har observeret, at den seneste ISAE 3402 type 2-erklæring er indhentet fra serviceunderleverandøren, og vi har foretaget inspektion heraf. Endvidere har vi observeret, at direktionen har udført sin kontrol som beskrevet i proceduren.	Ingen afvigelser konstateret.
4.1.5 Serviceunderleverandør - egne kontroller • Der foretages årligt kontrol af serviceleverandøren for at afdække, om serviceleverandøren stadig lever op til 9k Technologies APS' forventninger. Kontrollen godkendes af systemejer.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at kontrollen er udført som beskrevet i proceduren.	Ingen afvigelser konstateret.
4.1.6 Sikkerhedskopiering • Det kontrolleres, at backupservices virker, og at 9k Technologies ApS' udviklere modtager notifikation om resultatet af backupprocessen. Der foretages desuden kontrol af genskabelse af backup for at sikre, at den virker. Kontrollen godkendes hvert halve år af direktionen.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at der sker en daglig og komplet sikkerhedskopiering af systemer og data med besked om resultatet af denne sikkerhedskopiering til relevant personale. Vi har inspiceret dokumentation for retablering af database, der forløb problemfrit, og vi har observeret, at direktionen har udført kontrollen som beskrevet i proceduren.	Ingen afvigelser konstateret.

4.1 Generelle sikkerhedsbestemmelser

Kontrolmål

- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*
- *At beskytte mod tab af data.*
- *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*
- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.*
- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.1.7 Proceshåndbog • Der foretages kontrol af proceshåndbogen hvert halve år, hvor det kontrolleres, at de beskrevne processer er up-to-date, og om det stadig er dem, medarbejderne skal følge.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren og proceshåndbogen. Vi har observeret, at den halvårlige kontrol er udført i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
4.1.8 Change Management • Det kontrolleres hvert halve år, at ændringer i værktøjet har været igennem en procedure, hvor ændringerne evalueres af minimum en anden udvikler, før de lanceres i produktionsmiljøet. Derudover kontrolleres, at programmerede test har været afviklet. Kontrollen godkendes af systemejer.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, der beskriver change management processen for udvikling og vedligeholdelse af systemerne, herunder test og kontrol før overførsel til produktionsmiljø. Vi har observeret, at der alene er idriftsat afprøvede og godkendte systemændringer. Vi har observeret, at kontrollen er udført som beskrevet i proceduren.	Ingen afvigelser konstateret.
4.1.9 Drift • Der bliver halvårligt foretaget kontrol af, at serverens ydeevne stadig lever op til behovet. Kontrollen godkendes af direktionen.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at direktionen har udført kontrollen som beskrevet i proceduren.	Ingen afvigelser konstateret.

4.2 Autorisation og adgangskontrol

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.*
- *At forhindre uautoriseret adgang til systemer og applikationer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.2.1 Brugerrettigheder i systemerne • Værktøjerne indeholder tre roller (Leder, moderator og medarbejder), der tildeles ud fra om brugeren må forespørge inddatere og/eller slette oplysninger. • Der foretages årligt kontrol af implementeringen af rollefordelingen i værktøjerne, som godkendes af systemejer.	Vi har foretaget interview af passende personale. Vi har observeret, at værktøjerne indeholder flere roller med forskellige rettigheder, og at disse kan tildeles ud fra om brugeren må forespørge, inddatere eller slette oplysninger. Vi har foretaget inspektion af dokumentationen for kontrol af implementeringen af rollefordelingen i værktøjerne, herunder at antallet af brugere med lederrolle svarer til det antal, som der forefindes instruks på i henhold til de indgåede databehandleraftaler.	Ingen afvigelser konstateret.
4.2.2 Brugeradgange • Systemejer vurderer og godkender årligt alle medarbejderes adgangsprivilegier til produktionsserveren og kildekoden (medarbejderniveau). • Systemejer kontrollerer og godkender årligt, at adgangsrettighederne til systemerne er korrekte (systemniveau). • Det kontrolleres årligt og godkendes af systemejer, at det kun er udviklere, der har adgang til kode, servere og data.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at kontrollerne er udført som beskrevet i proceduren. Vi har foretaget inspektion af dokumentationen af kontroller, herunder påset, at alene autoriserede medarbejdere har adgang til produktionsserveren, kildekodens repositories og data.	Ingen afvigelser konstateret.
4.2.3 Fortrolighed • Systemejer kontrollerer årligt, at alle udviklere har underskrevet sikkerhedspolitikkontrakten. • Direktionen kontrollerer årligt, at alle medarbejdere, der er en del af udviklingsteamet, har underskrevet sikkerhedspolitikkontrakten.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at kontrollen er udført af systemejer og direktion som beskrevet i proceduren. Vi har foretaget inspektion af dokumentationen for de udførte kontroller.	Ingen afvigelser konstateret.

4.2 Autorisation og adgangskontrol

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.*
- *At forhindre uautoriseret adgang til systemer og applikationer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.2.4 Adgangskoder • Værktøjerne er opsat med adgangskoder i henhold til god it-skik, herunder registrering af afviste adgangsforsøg med blokering til følge efter et vist antal forsøg. • Det kontrolleres årligt og godkendes af systemejer, at værktøjerne er opsat med adgangskoder i henhold til god it-skik.	Vi har foretaget interview af passende personale. Vi har observeret anvendelsen af adgangskoder ved udtræk af de opsatte krav til validering af brugere (password-politik), der i overensstemmelse med god it-skik skal være minimum 8 karakterer og komplekst. Vi har observeret, at afviste afgangsforsøg registreres, og at brugeren vil blive blokeret efter 3 forsøg. Vi har inspiceret proceduren og dokumentationen af den udførte kontrol.	Ingen afvigelser konstateret.

4.3 Ind- og uddatamateriale

Kontrolmål

- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.3.1 Medarbejdererklæring • Det kontrolleres årligt, at alle medarbejdere i udviklingsteamet har underskrevet en erklæring om, at al hemmelig information, fx personoplysninger og adgangskoder, ikke bliver delt med andre. Kontrollen godkendes af direktionen.	Vi har foretaget interview af passende personale. Vi har inspiceret proceduren, og vi har observeret, at kontrollen er udført som beskrevet i proceduren. Vi har inspiceret de af medarbejderne afgivne sikkerhedspolitikkontrakter.	Ingen afvigelser konstateret.

4.4 Eksterne kommunikationsforbindelser

Kontrolmål

- *At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.4.1 Krypteret kommunikation • Kommunikationen mellem værktøjernes webapplikation og databaseserveren er krypteret med en anerkendt stærk krypteringsstandard. • Der foretages årligt en kontrol af forbindelserne til værktøjerne, produktionsserveren og kildekoden, for at kontrollere, at de stadig er krypteret. Denne kontrol godkendes af direktionen.	Vi har foretaget interview af passende personale. Vi har observeret, at kommunikationen mellem webapplikation og databaseserver er krypteret med en 256 byte SSL krypteret HTTPS forbindelse. Adgang til produktionsserveren sker ved brug af VPN og en krypteret SSH forbindelse. Vi har inspiceret proceduren, og vi har observeret, at direktionen har udført kontrollen som beskrevet i proceduren. Vi har foretaget inspektion af dokumentationen af den udførte kontrol.	Ingen afvigelser konstateret.

4.5 Logning

Kontrolmål

- *At sikre opdagelse af informationssikkerhedsbrud, undtagelser, fejl og lignende hændelser.*
- *At sikre registrering af alle anvendelse af personoplysninger.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
4.5.1 Logning • Værktøjerne er opsat med logning af alle anvendelser af personoplysninger, herunder oplysning om tidspunkt, bruger, anvendelsestype og personen. • Loggen opbevares i 6 måneder, hvorefter den slettes, medmindre andet fremgår af databehandleraftalen. • Hændelseslogningen til registrering af informationssikkerhedsbrud, undtagelser, fejl eller lignende opbevares og gennemgås regelmæssigt. • Der gennemføres en årlig kontrol af, at loggen udføres korrekt i henhold til sikkerhedsbekendtgørelsens § 19, stk. 1. Direktionen kontrollerer, at kontrollen er foretaget og godkender den.	Vi har foretaget interview af passende personale. Vi har observeret, at logning sker såvel ved adgang gennem webapplikationen som ved adgang til produktionsserveren, og at adgang til loggen alene er tildelt medarbejdere med et arbejdsbetinget behov herfor. Vi har observeret, at der ved adgang gennem webapplikationen registreres alle anvendelser af personoplysninger, og at loggen opbevares i 6 måneder, hvorefter den slettes, medmindre andet fremgår af databehandleraftalen. Vi har inspiceret proceduren og dokumentationen for den udførte kontrol af direktionen.	Ingen afvigelser konstateret.